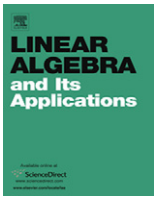
Linear Algebra and its Applications 435 (2011) 1956–1971

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa



The eigenstructure of finite field trigonometric transforms

J.B. Lima [a,*], R.M. Campello de Souza [b], D. Panario [c]

[a] Polytechnic School of Pernambuco, University of Pernambuco, Rua Benfica, 455, Madalena, Recife, PE 50750-470, Brazil
[b] Department of Electronics and Systems, Federal University of Pernambuco, Av. Acadêmico Hélio Ramos, S/N, 4° andar, Cidade Universitária, Recife, PE 50740-530, Brazil
[c] School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6

ARTICLE INFO

Article history:
Received 8 April 2010
Accepted 21 March 2011
Available online 21 April 2011

Submitted by R.A. Brualdi

AMS classification:
15A18
12E20
43A32
94A05

Keywords:
Eigenvalues
Eigenvectors
Finite fields
Trigonometric transforms

ABSTRACT

In this paper, we discuss the eigenstructure of finite field trigonometric transforms (FFTT). This transform family includes different types of cosine and sine transforms that correspond, in the finite field case, to the well known discrete cosine and sine transforms defined over the real numbers. More specifically, we determine the eigenvalues of the FFTT matrices and study their multiplicities. We propose procedures for constructing the associated eigenvectors. Applications of the developed theory to multiuser communication systems and error-correcting codes are also suggested.

1. Introduction

Transforms in finite fields have been studied and applied in many scenarios after Pollard defined the fast Fourier transform in a finite field [1]. In digital signal processing, for instance, these transforms are attractive because they avoid floating point operations and rounding errors [2]. Due to these characteristics, in comparison with real-valued mathematical tools, faster hardware implementations could be designed.

* Corresponding author. Tel.: +55 81 91140396; fax: +55 81 21268215.
E-mail addresses: juliano.bandeira@upe.poli.br (J.B. Lima), ricardo@ufpe.br (R.M.C. de Souza), daniel@math.carleton.ca (D. Panario).

0024-3795/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2011.03.031

Although finite field transforms have several theoretical particularities their development is usually guided by the existence of analogous transforms already defined over the real numbers. In this sense, after the Fourier transform, other finite field transforms were defined. The finite field Hartley transform (FFHT) was proposed in [3]; it has applications in digital multiplexing systems design, multiple access systems and multilevel spread spectrum of sequences. The finite field wavelet transform (FFWT) is another example. It has been applied in error-correcting coding and cryptography [4,5].

The trigonometric transforms, which compose another important class of transforms, were also defined in finite fields [6]. The family of finite field trigonometric transforms (FFTT) includes eight types of cosine transforms (FFCT) and eight types of sine transforms (FFST). Each type of FFTT can be obtained from specific symmetric extension procedures, applied to the finite field vector whose transform one desires to compute. Such a computation is commonly expressed by a matrix product between the vector and the transform matrix. In a general way, the study of the referred matrix helps the characterization of the respective transform, supporting the construction of fast algorithms and the establishment of relevant properties [7].

Encouraged by the above presented aspects, this paper has the main purpose of investigating the eigenstructure of the finite field trigonometric transform matrices. After the review of some mathematical preliminaries in the next section, the eigenvalues of the main FFTT types are studied in Sections 3, 4 and 5. Additionally, systematic procedures for obtaining eigenvectors of some of these transforms are shown. In Section 6, we suggest two applications for the developed theory. The first one is related to sequence separation. This approach, which is potentially useful in multiuser communication schemes, was preliminary investigated in [8]. In the second part of Section 6, we describe how to construct linear block codes based on the FFTT. The paper closes with some concluding remarks in Section 7.

2. Preliminaries

2.1. Finite field trigonometry

We review the main concepts related to finite field trigonometry [3]. In this paper, GF(q) represents a finite field with q elements.

Definition 1. The set of Gaussian integers over GF(p) is the set GI(p) $= \{a + jb, a, b \in \mathrm{GF}(p)\}$, where p is a prime such that $j^2 \equiv -1 \pmod p$ is a quadratic nonresidue over GF(p), i.e., $p \equiv 3 \pmod 4$.

The extension field GF(p^2) is isomorphic to the "complex" structure GI(p), whose elements $\zeta = a + jb$ have a "real" part $a = \Re\{\zeta\}$ and an "imaginary" part $b = \Im\{\zeta\}$ [7].

Definition 2. The unimodular set of GI(p) is the set of elements $\zeta = (a + jb) \in \mathrm{GI}(p)$, such that $a^2 + b^2 \equiv 1 \pmod p$.

Definition 3 (*finite field trigonometric functions*)**.** Let ζ be a unimodular element of GI(p), $p \equiv 3 \pmod 4$, with multiplicative order denoted by $\mathrm{ord}(\zeta)$. The finite field trigonometric functions cosine and sine related to ζ are computed modulo p, respectively, as

$$\cos_\zeta(x) := \frac{\zeta^x + \zeta^{-x}}{2} \tag{1}$$

and

$$\sin_\zeta(x) := \frac{\zeta^x - \zeta^{-x}}{2j}, \tag{2}$$

$x = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$.

Here, we use a notation slightly different from that established in [3]. [1] However, independently of this fact, the above finite field trigonometric functions hold properties similar to those of the standard real-valued trigonometric functions, such as *unit circle* and *addition of arcs*, for instance [3].

Lemma 1. *Let ζ be a unimodular element of* GI(p), $p \equiv 3 \pmod 4$, *with multiplicative order* $ord(\zeta) = N$. *The finite field cosine and sine functions are, respectively, computed by* $\cos_\zeta(x) = \Re\{\zeta^x\}$ *and* $\sin_\zeta(x) = \Im\{\zeta^x\}$, $x = 0, 1, \ldots, N-1$.

Proof. Using Eq. (1) and assuming $\zeta^x = c + jd$, $c, d \in$ GF(p), one has

$$\cos_\zeta(x) = \frac{(c+jd) + (c+jd)^{-1}}{2}.$$

Since $\zeta^x = c + jd$ is also unimodular, we may write $(c+jd)^{-1} = (c+jd)^* = c - jd$, where $(\cdot)^*$ denotes the "complex conjugate" of the argument. Therefore, the last equation can be rewritten as

$$\cos_k(i) = \frac{(c+jd) + (c-jd)}{2} = c = \Re\left\{\zeta^{ki}\right\}.$$

The proof that $\sin_\zeta(x) = \Im\{\zeta^x\}$ follows the same steps. □

2.2. Finite field trigonometric transforms

The discrete transforms defined over infinite fields are well-known. The discrete Fourier transform (DFT), for instance, became an essential resource in several application scenarios [9]. The finite field Fourier transform (FFFT), the first version of which was proposed by Pollard [1], is also a useful mathematical tool. In the context of signal processing, it can be applied on the computation of a linear convolution between a discrete-time signal and a filter [10]; in error-correcting coding, the FFFT can be used to describe block codes [11].

In this section, we present the main types of finite field trigonometric transforms. The construction of the FFTT is analogous to that one of the discrete trigonometric transforms [12]. The procedure, which is based on symmetric extensions of a sequence (or vector), leads to the definition of cosine and sine transforms. In the finite field framework, such transforms are, respectively, denoted by FFCT and FFST. [2]

In general, any FFTT of a sequence $\mathbf{x} = (x_i)$, $x_i \in$ GF(p), is a sequence $\mathbf{X} = (X_k)$, $X_k \in$ GI(p), obtained by the matrix equation

$$\mathbf{X} = \mathbf{x} \cdot \mathbf{M}^T. \tag{3}$$

In Eq. (3), $\mathbf{M}$ is the transform matrix. Its elements are computed according to the first column of Table 1, where the weight function β_r is given by

$$\beta_r = \begin{cases} \sqrt{2^{-1}} \pmod p, & r = 0 \text{ or } N, \\ 1, & r = 1, 2, \ldots, N-1. \end{cases}$$

The dimensions of $\mathbf{x}$, $\mathbf{X}$ and $\mathbf{M}$ are specified in the second column of this table, where the range on indexes i (row) and k (column) are shown. For the sake of simplicity, the cosine and sine transform matrices are identified as **FC** and **FS**, respectively. Besides the transform type, we also may include

[1] Originally, the finite field functions cosine and sine are related to $\angle\zeta^i$, the "arc" of ζ^i and called k-trigonometric functions. They are computed as $\cos_k(\angle\zeta^i) = (\zeta^{ki} + \zeta^{-ki})/2$ and $\sin_k(\angle\zeta^i) = (\zeta^{ki} - \zeta^{-ki})/2j$, for $i, k = 0, 1, \ldots, \mathrm{ord}(\zeta) - 1$, where the parameters i and k are, respectively, associated to the FFHT "time" and "frequency" domains.

[2] The first introduced FFTT was the type 2 finite field cosine transform [13]. Later, new definitions were given [6].

Table 1
Finite field cosine and sine transforms ($\zeta \in \mathrm{GI}(p)$, $p \equiv 3 \pmod 4$).

Transform matrix elements	Matrix dimension
$[\mathbf{FC}_1]_{i,k} = \sqrt{\frac{2}{N}}\,\beta_i\,\beta_k \cos_\zeta(ki)$	$i,k = 0,1,\ldots,N$
$[\mathbf{FC}_2]_{i,k} = \sqrt{\frac{2}{N}}\,\beta_k \cos_\zeta\left(k\left(i+\frac{1}{2}\right)\right)$	$i,k = 0,1,\ldots,N-1$
$[\mathbf{FC}_3]_{i,k} = \sqrt{\frac{2}{N}}\,\beta_i \cos_\zeta\left(\left(k+\frac{1}{2}\right)i\right)$	$i,k = 0,1,\ldots,N-1$
$[\mathbf{FC}_4]_{i,k} = \sqrt{\frac{2}{N}}\,\cos_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right)$	$i,k = 0,1,\ldots,N-1$
$[\mathbf{FS}_1]_{i,k} = \sqrt{\frac{2}{N}}\,\sin_\zeta(ki)$	$i,k = 1,2,\ldots,N-1$
$[\mathbf{FS}_2]_{i,k} = \sqrt{\frac{2}{N}}\,\beta_k \sin_\zeta\left(k\left(i+\frac{1}{2}\right)\right)$	$i = 0,1,\ldots,N-1$ $k = 1,2,\ldots,N$
$[\mathbf{FS}_3]_{i,k} = \sqrt{\frac{2}{N}}\,\beta_i \sin_\zeta\left(\left(k+\frac{1}{2}\right)i\right)$	$i = 1,2,\ldots,N$ $k = 0,1,\ldots,N-1$
$[\mathbf{FS}_4]_{i,k} = \sqrt{\frac{2}{N}}\,\sin_\zeta\left(\left(k+\frac{1}{2}\right)\left(i+\frac{1}{2}\right)\right)$	$i,k = 0,1,\ldots,N-1$

the dimensions of **M** in the notation.[3] Thus, the transform matrix denoted by $\mathbf{FC}_{N+1,1}$, for instance, is associated to the computation of **X**, the FFCT-1 of an $N+1$ length vector **x**.

The FFTT matrices are unitary. Since the matrices of types 1 and 4 FFTT are also symmetric, they correspond to involutions. Such matrices are elements of order 2 in the general linear group $\mathrm{GL}(N,\mathrm{GI}(p))$ [14]. In this group, an element of order r is a matrix of period r. The inverse FFCT-2 matrix, which is not symmetric, corresponds to the forward FFCT-3 matrix and vice-versa. This is also valid for the FFST-2 and the FFST-3. Additionally, we remark that, if ζ is unimodular, number theoretic transforms can be obtained, that is, transforms which map a vector with components in $\mathrm{GF}(p)$ on a transform vector with components in $\mathrm{GF}(p)$ (see Lemma 1).

3. Eigenstructure of type 1 FFTT

The finite field cosine and sine transforms of type 1 and the finite field Fourier transform have strongly connected eigenstructures. In order to demonstrate such a relationship, we denote the FFFT of a vector $\mathbf{x} = (x_i)$, $i = 0,\ldots,N-1$, $x_i \in \mathrm{GF}(p)$, by $\mathbf{X} = (X_k)$, $X_k \in \mathrm{GI}(p)$, $k = 0,\ldots,N-1$, which is computed by Eq. (3), with the transform matrix **M** substituted by the matrix $\mathbf{FF}_N$, the elements of which are

$$[\mathbf{FF}_N]_{i,k} = \sqrt{N^{-1}}\alpha^{ik}, \tag{4}$$

where $\alpha \in \mathrm{GI}(p)$ and $\mathrm{ord}(\alpha) = N$. Due to the scale factor $\sqrt{N^{-1}}$, the matrix $\mathbf{FF}_N$ is unitary.

Proposition 1. *The FFFT matrix has, at most, four distinct eigenvalues,* $\{1, -1, j, -j\}$*, whose multiplicities are presented in Table 2.*

Proposition 2. *Every eigenvector associated to the FFFT has even or odd symmetry. Even eigenvectors are related to the eigenvalues* 1 *or* -1*; odd eigenvectors are related to the eigenvalues* j *or* $-j$*.*

Proofs for Propositions 1 and 2 can be easily derived from results given in [15,16]. In this work, procedures for constructing FFFT eigenvectors are not discussed; we focused on FFCT and FFST transforms. We remark that an even symmetric vector $\mathbf{x}_e = (x_{e,i})$ holds the condition $x_{e,i} = x_{e,-i}$; similarly, an odd symmetric vector $\mathbf{x}_o = (x_{o,i})$ holds $x_{o,i} = -x_{o,-i}$. Based on the above results, the following propositions related to the eigenstructures of the FFCT-1 and the FFST-1 are presented.

Proposition 3. *The FFCT-*1 *and FFST-*1 *eigenvectors are constructed from the FFFT eigenvectors according to the following relations:*

[3] The transform symmetry should also be identified by the inclusion of the subscript e (even) or o (odd). However, since only even transforms are considered in the present work, the mentioned identification is omitted.

Table 2
Multiplicities of the eigenvalues of an $N \times N$ finite field Fourier transform matrix.

N	Mult. 1	Mult. -1	Mult. j	Mult. $-j$
$4n$	$n+1$	n	n	$n-1$
$4n+1$	$n+1$	n	n	n
$4n+2$	$n+1$	n	$n+1$	n
$4n+3$	$n+1$	$n+1$	$n+1$	n

- *If* $\mathbf{x} = [x_0, x_1, \ldots, x_{N-2}, x_{N-1}, x_{N-2}, \ldots, x_1]$ *is an even eigenvector of the matrix* $\mathbf{FF}_{2N-2}$, *then*

$$\hat{\mathbf{x}} = \left[x_0, \sqrt{2}x_1, \ldots, \sqrt{2}x_{N-2}, x_{N-1}\right] \tag{5}$$

  is an eigenvector of the matrix $\mathbf{FC}_{N,1}$, *i.e.,* $\mathbf{FC}_{N,1} \cdot \hat{\mathbf{x}}^T = \lambda\hat{\mathbf{x}}^T (\lambda = 1, -1)$.
- *If* $\mathbf{x} = [0, x_1, x_2, \ldots, x_N, 0, -x_N, -x_{N-1}, \ldots, -x_1]$ *is an odd eigenvector of the matrix* $\mathbf{FF}_{2N+2}$, *then*

$$\hat{\mathbf{x}} = \sqrt{2}\,[x_1, x_2, \ldots, x_N] \tag{6}$$

  is an eigenvector of the matrix $\mathbf{FS}_{N,1}$ *with associated eigenvalue* $j\lambda$, *i.e.,* $\mathbf{FS}_{N,1} \cdot \hat{\mathbf{x}}^T = j\lambda\hat{\mathbf{x}}^T$ $(\lambda = j, -j)$.

Proof. Our proof is similar to that of Proposition 3 in [17]. We consider the eigenvector $\mathbf{x}$ of the matrix $\mathbf{FF}_{2N-2}$, related to the eigenvalue $\lambda = 1$ or $\lambda = -1$. Equivalently, one has

$$\mathbf{FF}_{2N-2} \cdot \mathbf{x}^T = \lambda\mathbf{x}^T.$$

Using Eq. (4), which defines the FFFT matrix, the last equation is rewritten as

$$\sqrt{(2N-2)^{-1}} \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & \alpha^1 & \cdots & \cdots & \alpha^{2N-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{N-2} & \cdots & \cdots & \alpha^{(2N-3)\cdot(N-2)} \\ 1 & \alpha^{N-1} & \cdots & \cdots & \alpha^{(2N-3)\cdot(N-1)} \\ 1 & \alpha^{N-2} & \cdots & \cdots & \alpha^{(2N-3)\cdot(N-2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{2N-3} & \cdots & \cdots & \alpha^{(2N-3)^2} \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-2} \\ x_{N-1} \\ x_{N-2} \\ \vdots \\ x_1 \end{bmatrix} = \lambda \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-2} \\ x_{N-1} \\ x_{N-2} \\ \vdots \\ x_1 \end{bmatrix}.$$

Performing the matrix multiplication on the left hand side of the above equation, each component of the vector $\lambda\mathbf{x}^T$ is given by

$$\begin{aligned} \lambda x_m &= \sqrt{(2N-2)^{-1}} \left(x_0 + \sum_{k=1}^{N-2} \alpha^{km} x_k + \alpha^{m(N-1)} x_{N-1} + \sum_{k=1}^{N-2} \alpha^{m(2N-2-k)} x_k \right) \\ &= \sqrt{(2N-2)^{-1}} \left[x_0 + \alpha^{m(N-1)} x_{N-1} + \sum_{k=1}^{N-2} \left(\alpha^{km} + \alpha^{m(2N-2-k)} \right) x_k \right] \\ &= \sqrt{(2N-2)^{-1}} \left(x_0 + (-1)^m x_{N-1} + \sum_{k=1}^{N-2} 2\cos_\alpha(km) \right) x_k, \end{aligned}$$

Table 3
Multiplicities of the eigenvalues of type 1 $N \times N$ finite field cosine and sine transform matrices.

N	Mult. 1	Mult. -1
Odd	$\frac{N+1}{2}$	$\frac{N-1}{2}$
Even	$\frac{N}{2}$	$\frac{N}{2}$

for $m = 0, 1, \ldots, N-1$. We emphasize that $\alpha \in \mathrm{GI}(p)$, the element to which the finite field cosine function is related in the last equation, has multiplicative order $\mathrm{ord}(\alpha) = 2N-2$. Therefore,

$$\lambda x_m = \sqrt{\frac{2}{N-1}}\left[\frac{1}{2}x_0 + \frac{1}{2}(-1)^m x_{N-1} + \sum_{k=1}^{N-2} x_k \cos_\alpha(km)\right]. \tag{7}$$

To conclude the proof, we observe that Eq. (7) can also be obtained from the matrix equation

$$\lambda \begin{bmatrix} x_0 \\ \sqrt{2}x_1 \\ \vdots \\ \sqrt{2}x_{N-2} \\ x_{N-1} \end{bmatrix}$$

$$= \sqrt{\frac{2}{N-1}} \begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}} & \cdots & \frac{1}{\sqrt{2}} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \cos_\alpha(1) & \cdots & \cos_\alpha(N-2) & \frac{1}{\sqrt{2}}\cos_\alpha(N-1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{1}{\sqrt{2}} & \cos_\alpha(N-2) & \cdots & \cos_\alpha((N-2)(N-2)) & \frac{1}{\sqrt{2}}\cos_\alpha((N-2)(N-1)) \\ \frac{1}{2} & \frac{1}{\sqrt{2}}\cos_\alpha(N-1) & \cdots & \frac{1}{\sqrt{2}}\cos_\alpha((N-1)(N-2)) & \frac{1}{2}\cos_\alpha((N-1)(N-1)) \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ \sqrt{2}x_1 \\ \vdots \\ \sqrt{2}x_{N-2} \\ x_{N-1} \end{bmatrix},$$

which corresponds to $\lambda\hat{\mathbf{x}} = \mathbf{FC}_{N,1} \cdot \hat{\mathbf{x}}$. Therefore, λ is also an eigenvalue of the FFCT-1 transform matrix and $\hat{\mathbf{x}} = \left[x_0, \sqrt{2}x_1, \ldots, \sqrt{2}x_{N-2}, x_{N-1}\right]$ is its respective eigenvector. The demonstration for the FFST-1 is analogous. □

Proposition 4. *The FFCT-1 and the FFST-1 matrices have only the eigenvalues* 1 *and* -1. *Their multiplicities are presented in Table 3.*

Proof. From Proposition 3, we know that the eigenvectors of the matrix $\mathbf{FC}_{N,1}$ are related to even eigenvectors of the matrix $\mathbf{FF}_{2N-2}$. If N is even, it can be written as $N = 2(N'+1)$, where $N' \geqslant 0$ is an integer. Hence, $2N-2 = 4N'+2$. In this case, by observing Table 2, we verify that the multiplicities of the eigenvalues 1 and -1, respectively, denoted by $\#(1)$ and $\#(-1)$, are $\#(1) = \#(-1) = N'+1 = N/2$. If N is odd, it can be written as $N = 2N'+1$, which gives $2N-2 = 4N'$. In this case, one has $\#(1) = N'+1 = (N+1)/2$ and $\#(-1) = N' - 1 = (N-1)/2$. The results for the FFST-1 can be proved using analogous arguments. □

The above proof is similar to that presented for Proposition 4 in [17]. As we previously remarked, the FFCT-1 is involutive, i.e., $(\mathbf{FC}_{N,1})^2 = \mathbf{I}_N$, where $\mathbf{I}_N$ is the $N \times N$ identity matrix. Hence, the eigenvalues of $\mathbf{FC}_{N,1}$ can also be obtained from the solutions of $\lambda^2 = 1$, i.e., $\{-1, 1\}$. The same argument is valid for $\mathbf{FS}_{N,1}$.

4. Eigenstructure of type 4 FFTT

In this section, the eigenstructures of the FFCT-4 and the FFST-4 are discussed. This requires a new definition: the generalized finite field Fourier transform (GFFFT). Initially, we introduce the GFFFT and analyze its eigenstructure. Propositions concerning the eigenstructures of type 4 FFTT are then derived.

4.1. The generalized finite field Fourier transform

The GFFFT of a vector $\mathbf{x} = (x_i)$, $i = 0, 1, \ldots, N-1$, $x_i \in \mathrm{GF}(p)$, is a vector $\mathbf{X} = (X_k)$, $k = 0, 1, \ldots, N-1$, $X_k \in \mathrm{GI}(p)$, computed by Eq. (3), with the matrix $\mathbf{M}$ substituted by

$$\mathbf{FF}_{N,G} = \sqrt{N^{-1}}\alpha^{\left(i+\frac{1}{2}\right)\left(k+\frac{1}{2}\right)}, \tag{8}$$

where $\alpha \in \mathrm{GI}(p)$ and $\mathrm{ord}(\alpha) = N$. The inverse of $\mathbf{FF}_{N,G}$ is

$$(\mathbf{FF}_{N,G})^{-1} = \sqrt{N^{-1}}\alpha^{-\left(i+\frac{1}{2}\right)\left(k+\frac{1}{2}\right)}. \tag{9}$$

In what follows, some properties used for studying the eigenstructure of the $\mathbf{FF}_{N,G}$ are presented.

Property 1. *Let* $\mathbf{J}$ *be an* $N \times N$ *anti-diagonal matrix, i.e., a matrix where all the entries are zero except those on the anti-diagonal, such that every nonzero element equals* 1. *Then,* $(\mathbf{FF}_{N,G})^2 = -\mathbf{J}$.

The proof of the above property is similar to the proof presented for the Fact 1 in [18]. Based on this property and denoting by $x_i \overset{G}{\longleftrightarrow} X_k$ the relation between $\mathbf{x}$ and its generalized finite field Fourier transform $\mathbf{X}$, the relation $X_i \overset{G}{\longleftrightarrow} -x_{-k-1}$ is valid.

In order to analyze the GFFFT of symmetric vectors, differently from the FFFT, we consider even symmetric vectors $\mathbf{x}_e$ holding the condition $x_{e,i} = x_{e,-i-1}$. They can be constructed from any vector $\mathbf{x}$ by $x_{e,i} = \mathcal{E}\{x_i\} = 2^{-1}(x_i + x_{-i-1})$; symmetric odd vectors hold $x_{o,i} = -x_{o,-i-1}$ and they can be obtained by $x_{o,i} = \mathcal{O}\{x_i\} = 2^{-1}(x_i - x_{-i-1})$. Naturally, in the construction of the vectors $\mathbf{x}_e$ and $\mathbf{x}_o$, the computations are done modulo a prime number p.

Property 2. *If* $x_i \overset{G}{\longleftrightarrow} X_k$, *then* $\mathcal{E}\{x_i\} \overset{G}{\longleftrightarrow} \mathcal{E}\{X_k\}$ *and* $\mathcal{O}\{x_i\} \overset{G}{\longleftrightarrow} \mathcal{O}\{X_k\}$.

This property can be demonstrated using Eq. (8) and the established symmetry conditions.

Proposition 5. *The GFFFT matrix has, at most, four distinct eigenvalues,* $\{1, -1, j, -j\}$, *the multiplicities of which are presented in Table 4.*

Proof. Using Property 1, we know that $(\mathbf{FF}_{N,G})^4 = \mathbf{I}_N$. Consequently, the eigenvalues of $\mathbf{FF}_{N,G}$ correspond to the solutions of $\lambda^4 = 1$, i.e., $\{1, -1, j, -j\}$. Their multiplicities are determined using a proof similar to that presented for the Fact 3 in [18]. □

The form of the GFFFT matrix eigenvectors is described in the following propositions. Based on Property 2 and on [19], where the eigenstructure of the discrete Fourier transform (DFT) is analyzed, we present a systematic procedure for constructing $\mathbf{FF}_{N,G}$ eigenvectors.

Table 4
Multiplicities of the eigenvalues of an $N \times N$ generalized finite field Fourier transform matrix.

N	Mult. 1	Mult. -1	Mult. j	Mult. $-j$
$4n$	n	n	n	n
$4n+1$	n	n	n	$n+1$
$4n+2$	$n+1$	n	n	$n+1$
$4n+3$	$n+1$	n	$n+1$	$n+1$

Proposition 6. *Any eigenvector* $\mathbf{x}$ *of the GFFFT matrix satisfies one of the following conditions:*

- *The vector* $\mathbf{x}$ *is even symmetric, i.e.,* $\mathbf{J}\cdot\mathbf{x}=\mathbf{x}$*, and its respective eigenvalue is either* j *or* $-j$*.*
- *The vector* $\mathbf{x}$ *is odd symmetric, i.e.,* $\mathbf{J}\cdot\mathbf{x}=-\mathbf{x}$*, and its respective eigenvalue is either* 1 *or* -1*.*

Proof. Since $\mathbf{x}$ is an eigenvector of $\mathbf{FF}_{N,G}$, the equality $\mathbf{FF}_{N,G}\cdot\mathbf{x}=\lambda\mathbf{x}$ is valid. Multiplying both sides of the last expression by $\mathbf{FF}_{N,G}$ and using the fact that $(\mathbf{FF}_{N,G})^2=-\mathbf{J}$, one obtains

$$-\mathbf{J}\cdot\mathbf{x}=\lambda^2\mathbf{x}. \tag{10}$$

If $\lambda=\pm1$, Eq. (10) is reduced to $-\mathbf{J}\cdot\mathbf{x}=\mathbf{x}$, which means that $\mathbf{x}$ has odd symmetry; if $\lambda=\pm j$, Eq. (10) is reduced to $\mathbf{J}\cdot\mathbf{x}=\mathbf{x}$, which means that $\mathbf{x}$ has even symmetry. □

Proposition 7. *The eigenvectors of the GFFFT matrix are constructed according to the following rules. If* $x_i \overset{G}{\longleftrightarrow} X_k$*, then:*

- *the even symmetric vector* $\mathbf{x}=\mathcal{E}\{x_i\}\mp j\mathcal{E}\{X_i\}$ *is an eigenvector of the matrix* $\mathbf{FF}_{N,G}$ *associated to the eigenvalue* $\lambda=\pm j$*;*
- *the odd symmetric vector* $\mathbf{x}=\mathcal{O}\{x_i\}\pm\mathcal{O}\{X_i\}$ *is an eigenvector of the matrix* $\mathbf{FF}_{N,G}$ *associated to the eigenvalue* $\lambda=\pm1$*.*

Proof. Using Properties 1 and 2, and the previously introduced notation, the relationship between $\mathcal{E}\{x_i\}\mp j\mathcal{E}\{X_i\}$ and its GFFFT can be expressed as:

$$\mathcal{E}\{x_i\}\mp j\mathcal{E}\{X_i\} \overset{G}{\longleftrightarrow} \mathcal{E}\{X_k\}\pm j\mathcal{E}\{x_{-k-1}\}.$$

Since $\mathcal{E}\{x_{-k-1}\}=\mathcal{E}\{x_k\}$, the last equation can be written as

$$\mathcal{E}\{x_i\}\mp j\mathcal{E}\{X_i\} \overset{G}{\longleftrightarrow} \pm j\left(\mathcal{E}\{x_k\}\mp j\mathcal{E}\{X_k\}\right)$$

from which the result follows. Analogously, we have

$$\mathcal{O}\{x_i\}\pm\mathcal{O}\{X_i\} \overset{G}{\longleftrightarrow} \mathcal{O}\{X_k\}\mp\mathcal{O}\{x_{-k-1}\}.$$

Since $\mathcal{O}\{x_{-k-1}\}=-\mathcal{O}\{x_k\}$, the last equation can be written as

$$\mathcal{O}\{x_i\}\pm\mathcal{O}\{X_i\} \overset{G}{\longleftrightarrow} \pm\left(\mathcal{O}\{x_k\}\pm\mathcal{O}\{X_k\}\right),$$

from which the result follows. □

4.2. Eigenvalues and eigenvectors of type 4 FFTT

Based on the GFFFT eigenstructure, the following propositions related to the eigenstructures of the FFCT-4 and the FFST-4 are presented.

Proposition 8. *The eigenvectors of the FFCT-4 and the FFST-4 matrices are constructed from the eigenvectors of the GFFFT matrix according to the following relations:*

- *If* $\mathbf{x}=[x_0,\ldots,x_{N-1},-x_{N-1},\ldots,-x_0]$ *is an odd eigenvector of the matrix* $\mathbf{FF}_{2N,G}$*, then*

$$\hat{\mathbf{x}}=[x_0,\ldots,x_{N-1}] \tag{11}$$

is an eigenvector of the matrix $\mathbf{FC}_{N,4}$*.*

Table 5
Multiplicities of the eigenvalues of an $N \times N$ type IV finite field cosine or sine transform matrix.

N	Mult. 1	Mult. -1
Odd	$\frac{N+1}{2}$	$\frac{N-1}{2}$
Even	$\frac{N}{2}$	$\frac{N}{2}$

- *If* $\mathbf{x} = [x_0, \ldots, x_{N-1}, x_{N-1}, \ldots, x_0]$ *is an even eigenvector of the matrix* $\mathbf{FF}_{2N,G}$*, then*

$$\hat{\mathbf{x}} = [x_0, \ldots, x_{N-1}] \tag{12}$$

is an eigenvector of the matrix $\mathbf{FS}_{N,4}$.

The proof of the above proposition is based on the same principles applied to demonstrate Proposition 3.

Proposition 9. *The FFCT-4 and the FFST-4 transform matrices have only the eigenvalues* 1 *and* -1*. Their multiplicities are presented in Table 5.*

The proof of the above proposition is similar to that of Proposition 4.

5. Types 2 and 3 FFTT eigenstructure

Since types 2 and 3 FFTT matrices are not symmetric, in order to analyze their eigenstructures, it is not possible to use arguments similar to those applied to types 1 and 4 FFTT. In fact, the eigenstructure of the real-valued types 2 and 3 trigonometric transforms remains unclear, being restricted to some conjectures supported by numerical simulations [20]. In this section, we also discuss a conjecture and investigate some aspects concerning the eigenstructure of the mentioned transforms in the finite field case.

The conventional procedure for obtaining the eigenvalues of a matrix consists in evaluating the roots of its characteristic polynomial. Since the FFTT matrices are orthogonal, the following theorem is valid.

Theorem 1. *The characteristic polynomial of an orthogonal matrix modulo p is a reciprocal polynomial* $f(\lambda)$.

Proof. Let $\mathbf{M}$ be an $N \times N$ orthogonal matrix with characteristic polynomial $f(\lambda) = \det(\mathbf{M} - \lambda\mathbf{I})$. We want to demonstrate that $f(\lambda) = \pm\lambda^N p(1/\lambda)$. Since $\mathbf{M}^{-1} = \mathbf{M}^T$, one has $\mathbf{M} - \lambda\mathbf{I} = -\lambda\mathbf{M}(\mathbf{M}^T - \mathbf{I}/\lambda)$. Considering the determinants on both sides of the last equation and using the fact that $\det(\mathbf{M}) = \det(\mathbf{M}^T) = \pm 1$ and $\det(\lambda\mathbf{M}) = \lambda^N \det(\mathbf{M})$, we obtain

$$\det(\mathbf{M} - \lambda\mathbf{I}) = \pm\lambda^N \det\left(\mathbf{M} - \frac{1}{\lambda}\mathbf{I}\right). \quad \square$$

The polynomial $f(\lambda)$ is also called palindromic, if $f(\lambda) = \lambda^N f(1/\lambda)$, or anti-palindromic, if $f(\lambda) = -\lambda^N f(1/\lambda)$. The computation of the roots of such polynomials is simplified by the use of a variable substitution method reducing its degree by half [21]. Therefore, it is possible to use closed formulas to evaluate the roots of palindromic polynomials with degrees up to 10. In this extreme case, after excluding roots $\pm 1 \pmod{p}$, the degree is reduced to 4. For $f(\lambda)$ with degree greater than 10, factorization techniques are used [22].

In [20], Cariolaro et al. used numerical tests to obtain eigenvalue constellations of the DCT-2 matrix and observed that the tendency of distinctness among these eigenvalues is preserved as N increases. In the finite field context, even if the elements of an FFCT-2 matrix are in a prime field, the most

part of the corresponding eigenvalues lies in extension fields, which makes harder the realization of tests similar to those mentioned [23]. Thus, we consider the fact that the matrices of a specific type of trigonometric transform have the same structure and symmetry properties (independently of the field being considered). This can be verified by comparing the expressions of the FFCT-2 and DCT-2. Naturally, this equivalence of structures is also verified in the coefficients of the respective characteristic polynomials and, consequently, in the roots of such polynomials. This lead us to conjecture that all eigenvalues of the FFCT-2 transform matrix are also distinct. The same argument is used for the FFCT-3, FFST-2 and FFST-3.

The period of the matrices $\mathbf{FC}_{N,2}$, $\mathbf{FC}_{N,3}$, $\mathbf{FS}_{N,2}$ and $\mathbf{FS}_{N,3}$ can be investigated by writing them in diagonal form. Let us consider again the FFCT-2 matrix and write it as $\mathbf{FC}_{N,2} = \mathbf{U}\Lambda\mathbf{U}^*$ ($\mathbf{U}$ is a unitary matrix, the columns of which are eigenvectors of $\mathbf{FC}_{N,2}$, and $\mathbf{U}^*$ is its conjugate transpose; Λ is a diagonal matrix whose elements are the eigenvalues of $\mathbf{FC}_{N,2}$). Since $\mathbf{U}^*\mathbf{U} = \mathbf{I}$, powers of $\mathbf{FC}_{N,2}$ can be computed from powers of Λ, which are computed taking the respective power of each element in its main diagonal. Hence, the relation $(\mathbf{FC}_{N,2})^r = \mathbf{U}\Lambda^r\mathbf{U}^*$ holds. The least positive integer r such that $(\mathbf{FC}_{N,2})^r = \mathbf{I}$ also implies $\Lambda^r = \mathbf{I}$. From this condition, we conclude that the period r is the least common multiple among the multiplicative orders of the eigenvalues of $\mathbf{FC}_{N,2}$. For types 2 and 3 real-valued trigonometric transforms, there is a conjecture stating that no such r exists [20]. By definition, the periods of types 2 and 3 matrices are said to be zero. Naturally, for the FFTT case, r is always finite.

In summary, we can assert that the computation of types 2 and 3 FFTT matrices eigenvalues requires the computation of the roots of the respective characteristic polynomials. In this way, related eigenvectors can be constructed.

6. Applications

In this section, we discuss some potential applications for the theory developed throughout this paper. In a first scenario, the possibility of separating eigenvectors that have been added to each other is explored. This is achieved due to the orthogonality between eigenspaces defined by different eigenvalues of a finite field trigonometric transform matrix. The usage of such a separation procedure in multiuser communication schemes is suggested. In another scenario, the studied eigenstructures can be applied to error-correcting coding. More specifically, we propose to use the eigenvectors of an FFTT matrix as the codewords of a linear block code. As we will show, the parameters of the obtained code depend on the multiplicity of the used eigenvalues.

6.1. Sequence separation

In communication theory, the problem of separating information coming from different sources, after they are "mixed" under some assumptions, has been extensively studied [24,25]. Among different techniques for recovering the data originally transmitted by each user, a particularly interesting case is the separation without explicit knowledge of the information related to each source (or user). When different users share the same frequency band at the same time, well established techniques perform such a separation using statistical properties of sequences and codes used as "digital carriers".

Here, using the above described scenario as reference, we show how the FFTT eigenstructure can be used for sequence separation. We consider a noise free finite field adder channel which is synchronously shared by different users [26]. The procedure consists in associating an eigenvalue and, therefore, a set of eigenvectors of a given FFTT to each user. The information to be sent by an user is mapped on such eigenvectors. Since eigenvectors related to different eigenvalues are orthogonal, after being summed by the channel, they can be recovered by solving a linear system of equations. This scheme is illustrated in the following subsections.

6.1.1. 2-User scheme

With the purpose of presenting a 2-user scheme, we consider an $N \geqslant 2$ length FFCT-1, although any other FFTT whose transform matrix has at least 2 distinct eigenvalues can be used. As demonstrated in Section 3, the FFCT-1 matrix has eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -1$. We associate to these eigenvalues

and to users 1 and 2, respectively, the eigenvectors $\mathbf{x}_1 = (x_{1,i})$ and $\mathbf{x}_2 = (x_{2,i})$, which are constructed according to Proposition 3.

From the vector $\mathbf{y} = (y_i)$ given by

$$y_i = x_{1,i} + x_{2,i}, \tag{13}$$

where "+" denotes componentwise addition modulo p, it is possible to recover the user sequences. By computing $\mathbf{Y} = (Y_k) = \mathbf{FC}_{N,1} \cdot \mathbf{y}^T$, one has

$$Y_k = \lambda x_{1,i} + \lambda_2 x_{2,i} = x_{1,i} - x_{2,i}. \tag{14}$$

Solving the linear system formed by Eqs. (13) and (14), the user sequences are recovered from the modulo p equations $x_{1,i} = (y_i + Y_i)/2$ and $x_{2,i} = (y_i - Y_i)/2$.

6.1.2. 4-User scheme

According to our previous discussions, we must choose types 2 or 3 FFTT for constructing a 4-user scheme. Moreover, if a transform over GF(p) is chosen, the eigenvalues used for implementing such a scheme should also be located in GF(p), in order to avoid computations in extension fields. As an example, let us consider the 4-length FFCT-2 over GF(127). If the transform matrix is constructed using the unimodular element $\zeta = 119 + j119$, its eigenvalues are $\lambda_1 = 1$, $\lambda_2 = 20$, $\lambda_3 = 108$ and $\lambda_4 = 126$; the user sequences are, respectively, the eigenvectors $\mathbf{x}_1 = (x_{1,i})$, $\mathbf{x}_2 = (x_{2,i})$, $\mathbf{x}_3 = (x_{3,i})$ and $\mathbf{x}_4 = (x_{4,i})$.

Analogously to the 2-user scheme, the adder channel produces the vector $\mathbf{y} = (y_i)$. By computing successive transforms of $\mathbf{y}$, we have

$$\begin{aligned}
\mathbf{Y^{(1)}} &= \left(Y_k^{(1)}\right) = \mathbf{FC}_{N,2} \cdot \mathbf{y}^T, \\
\mathbf{Y^{(2)}} &= \left(Y_k^{(2)}\right) = (\mathbf{FC}_{N,2})^2 \cdot \mathbf{y}^T, \\
\mathbf{Y^{(3)}} &= \left(Y_k^{(3)}\right) = (\mathbf{FC}_{N,2})^3 \cdot \mathbf{y}^T.
\end{aligned}$$

Hence, the following linear system of equations is obtained:

$$\begin{cases}
x_{1,i} + x_{2,i} + x_{3,i} + x_{4,i} & = y_i \\
\lambda_1 x_{1,i} + \lambda_2 x_{2,i} + \lambda_3 x_{3,i} + \lambda_4 x_{4,i} & = Y_i^{(1)} \\
\lambda_1^2 x_{1,i} + \lambda_2^2 x_{2,i} + \lambda_3^2 x_{3,i} + \lambda_4^2 x_{4,i} & = Y_i^{(2)} \\
\lambda_1^3 x_{1,i} + \lambda_2^3 x_{2,i} + \lambda_3^3 x_{3,i} + \lambda_4^3 x_{4,i} & = Y_i^{(3)}.
\end{cases}$$

Substituting the values of λ_i, $i = 1, \ldots, 4$, in the above system, we have

$$\begin{cases}
x_{1,i} + x_{2,i} + x_{3,i} + x_{4,i} & = y_i \\
x_{1,i} + 20\,x_{2,i} + 108\,x_{3,i} + 126\,x_{4,i} & = Y_i^{(1)} \\
x_{1,i} + 19\,x_{2,i} + 107\,x_{3,i} + x_{4,i} & = Y_i^{(2)} \\
x_{1,i} + 126\,x_{2,i} + 126\,x_{3,i} + 126\,x_{4,i} & = Y_i^{(3)},
\end{cases}$$

the solution of which is

$$\begin{aligned}
x_{1,i} &= 64\,y_i + 64\,Y_i^{(3)} \\
x_{2,i} &= 49\,y_i + 36\,Y_i^{(1)} + 78\,Y_i^{(2)} + 91\,Y_i^{(3)} \\
x_{3,i} &= 36\,y_i + 49\,Y_i^{(1)} + 91\,Y_i^{(2)} + 78\,Y_i^{(3)} \\
x_{4,i} &= 106\,y_i + 42\,Y_i^{(1)} + 85\,Y_i^{(2)} + 21\,Y_i^{(3)}.
\end{aligned}$$

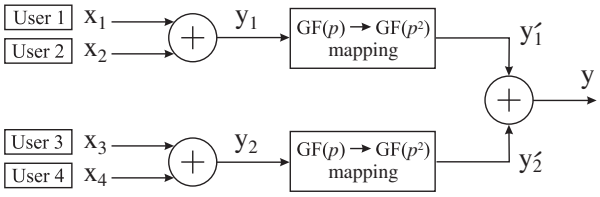


Fig. 1. A two-level hierarchy of the eigenstructure based multiuser communication.

Therefore, from $\mathbf{y}$, we obtain $\mathbf{Y^{(1)}}$, $\mathbf{Y^{(2)}}$ and $\mathbf{Y^{(3)}}$ and use the above equations for recovering each user sequence. Following these principles, schemes with a larger number of simultaneous users can be implemented.

6.1.3. Discussion

Since we assume the eigenvalues used in a specific scheme are fixed, the system of equations from which the user sequences are recovered has to be solved only once. In fact, the solution has to be applied again for each received vector $\mathbf{y}$. However, such a solution is already known. Furthermore, the computational complexity of this procedure can be estimated in terms of arithmetic operations. In order to do this, we just have to count the number of additions and multiplications required by (1) the solution of the system of equations and (2) the computation of the FFTT of $\mathbf{y}$ [27].

As we remarked, the proposed sequence separation method restricts the number of simultaneous users of a scheme to the number of distinct eigenvalues of the used FFTT. However, similarly to usual multiplexing techniques, it is possible to implement hierarchic schemes. As an example, let us consider the 4-user scheme presented in Figure 1, implemented by using transforms with only 2 distinct eigenvalues. In the figure, the eigenvectors $\mathbf{x}_1$ and $\mathbf{x}_2$ are, respectively, related to the eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -1$ of $\mathbf{FC}_{2,1}$ (the 2×2 FFCT-1 matrix) over GF(p). According to the 2-user scheme described in Section 6.1.1, $\mathbf{y}_1$ can be any 2-length vector over GF(p). More precisely, there are p^2 different possibilities for $\mathbf{y}_1$. If we employ the same 2-user scheme for multiplexing users 3 and 4, obviously, $\mathbf{y}_1$ and $\mathbf{y}_2$ cannot be added directly to form a new hierarchic level. However, we can create a mapping which relates each vector $\mathbf{y}_1$ (resp. $\mathbf{y}_2$) to an eigenvector $\mathbf{y}'_1$ (resp. $\mathbf{y}'_2$) associated to the eigenvalue $\lambda_1 = 1$ (resp. $\lambda_2 = -1$) of $\mathbf{FC_{2,1}}$ over GF(q), $q \geqslant p^2$, and produce the vector $\mathbf{y} = \mathbf{y'_1} + \mathbf{y'_2}$. The four users sequences can be recovered by separating $\mathbf{y}'_1$ and $\mathbf{y}'_2$ from $\mathbf{y}$, applying reverse mappings and, finally, separating $\mathbf{x}_1$ and $\mathbf{x}_2$ from $\mathbf{y_1}$, and $\mathbf{x}_3$ and $\mathbf{x}_4$ from $\mathbf{y_2}$. These ideas can be extended by using transforms defined over different finite fields. Thus, even if an FFTT with a restrict number of distinct eigenvalues is used, the strategy of creating new hierarchic levels allows to multiplex a larger number of users.

Although the proposed sequence separation technique is performed by using modular arithmetic, in a practical scenario, the noise that possibly corrupts the transmitted sequences is analog. If the sequences were over GF(7), for instance, we should use 7 quantization levels, so that, even if the channel was noisy, the technique should work up to a certain level of signal-to-noise ratio (SNR). Signals could be transmitted by using a 7-ary pulse amplitude modulation (PAM), the performance of which would be essentially the same of an 8-ary PAM [28]. This indicates that the FFTT data multiplexing system is practical for noisy channels. Naturally, its performance could be improved by the use of error-correcting coding.

Other interesting aspects of the multiuser communication based on the eigenstructures of the FFTT are revealed by performing a comparison with the direct sequence code division multiple access (DS-CDMA) [24,25]. In this sense, the above presented schemes can be viewed as DS-CDMA where the spreading sequences (user signatures) are eigenvectors of a finite field transform, instead of Walsh codes or pseudo-noise sequences. Different from DS-CDMA receivers, which use autocorrelation and cross-correlation properties of the spreading sequences, in our approach, the successful separation of each user sequence depends on the orthogonality between distinct eigenspaces. Moreover, since DS-

CDMA uses binary sequences, it increases simultaneously the transmission rate and the bandwidth by the same factor, keeping thus the spectral efficiency unchanged. Our approach exploits orthogonality properties of non-binary (multilevel) sequences over finite fields. The main advantage of this technique regarding classical multiple access digital schemes is its better spectral efficiency, in particular, for channels supporting a high SNR [29].

6.2. Error-correcting codes

In this section, we explain how to construct linear block codes based on the FFTT. We also discuss the existing relationship between the eigenstructure of such transforms and the parameters of the corresponding code. In fact, given any linear transform matrix, it is possible to apply a systematic procedure and obtain a linear block code. This idea was introduced by Campello de Souza et al. in [30], where the construction of codes based on the finite field Fourier transform was analyzed. What is special about using FFTT or any other finite field transform for that matter, is that we are constructing, in a systematic way, a family of linear block codes instead of a single isolated example. With the purpose of demonstrating how the referred procedure works, let us consider the pair $\mathbf{x} \leftrightarrow \mathbf{X}$, such that $\mathbf{x}$ is an eigenvector related to the eigenvalue λ of an N-length transform whose matrix is $\mathbf{M}$. Thus, one has

$$\mathbf{M} \cdot \mathbf{x} = \lambda \mathbf{x}$$

and, consequently,

$$(\mathbf{M} - \lambda \mathbf{I}) \cdot \mathbf{x} = 0.$$

In the above equation, the matrix $\mathbf{M} - \lambda \mathbf{I}$ performs a role equivalent to that of the parity-check matrix $\mathbf{H}$ of a linear block code of length $n = N$ and dimension k, such that

$$n - k = \operatorname{rank}(\mathbf{M} - \lambda \mathbf{I}).$$

If we scale the matrix $\mathbf{M} - \lambda \mathbf{I}$, the standard form of the parity-check matrix is obtained, i.e., $\mathbf{H} = [\mathbf{I}_{n-k} | \mathbf{P}]$, where $\mathbf{P}$ is determined by the parity equations of the code. The generator matrix in the form $\mathbf{G} = [-\mathbf{P}^T | \mathbf{I}_k]$ can also be obtained [31].

Naturally, if a transform over GF(p) is used, a p-ary code is generated. Since the codewords of a code generated by the above described procedure are the eigenvectors related to an eigenvalue λ, the number of different codes constructed from a given transform matrix equals the number of distinct eigenvalues of this matrix. Therefore, considering transforms of length N, from a finite field Fourier transform matrix, we can construct 4 different codes (see Proposition 1); from a finite field trigonometric transform of type 1 or 4, we can construct 2 different codes (see Propositions 4 and 9); from a finite field trigonometric transform of type 2 or 3, according to the conjecture presented in Section 5, we can construct N different codes.

6.2.1. Code parameters

In a general way, a code constructed from a transform matrix $\mathbf{M}$ is denoted by $\mathbf{M}^{\lambda}(n, k, d)$. The block length n of the code is the length of the transform computed by the matrix $\mathbf{M}$; the code dimension k is the multiplicity of the eigenvalue λ, since this is the dimension of the subspace defined by the eigenvectors related to λ [16].

In order to clarify the above presented concepts, we develop a small example. In what follows, we consider the FFCT-1 over GF(113). If we choose the unimodular element $\zeta = 17 + 27j$, a transform of length $N = 8$ is computed by the matrix

$$\mathbf{FC}_1 = \begin{bmatrix} 52 & 53 & 53 & 53 & 53 & 53 & 53 & 52 \\ 53 & 73 & 5 & 97 & 16 & 108 & 40 & 60 \\ 53 & 5 & 16 & 40 & 40 & 16 & 5 & 53 \\ 53 & 97 & 40 & 108 & 5 & 73 & 16 & 60 \\ 53 & 16 & 40 & 5 & 5 & 40 & 16 & 53 \\ 53 & 108 & 16 & 73 & 40 & 97 & 5 & 60 \\ 53 & 40 & 5 & 16 & 16 & 5 & 40 & 53 \\ 52 & 60 & 53 & 60 & 53 & 60 & 53 & 61 \end{bmatrix}.$$

Using the eigenvalue $\lambda = 1$, the parity-check matrix

$$\mathbf{H} = \mathbf{FC}_1 - \mathbf{I} = \begin{bmatrix} 51 & 53 & 53 & 53 & 53 & 53 & 53 & 52 \\ 53 & 72 & 5 & 97 & 16 & 108 & 40 & 60 \\ 53 & 5 & 15 & 40 & 40 & 16 & 5 & 53 \\ 53 & 97 & 40 & 107 & 5 & 73 & 16 & 60 \\ 53 & 16 & 40 & 5 & 4 & 40 & 16 & 53 \\ 53 & 108 & 16 & 73 & 40 & 96 & 5 & 60 \\ 53 & 40 & 5 & 16 & 16 & 5 & 39 & 53 \\ 52 & 60 & 53 & 60 & 53 & 60 & 53 & 60 \end{bmatrix}$$

is obtained. The scaled version of the above matrix is

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 45 & 6 & 13 & 75 \\ 0 & 1 & 0 & 0 & 21 & 66 & 74 & 100 \\ 0 & 0 & 1 & 0 & 82 & 56 & 47 & 6 \\ 0 & 0 & 0 & 1 & 21 & 31 & 21 & 68 \end{bmatrix}$$

and, consequently, the code generator matrix is

$$\mathbf{G} = \begin{bmatrix} 68 & 92 & 31 & 92 & 1 & 0 & 0 & 0 \\ 107 & 47 & 57 & 82 & 0 & 1 & 0 & 0 \\ 100 & 39 & 66 & 92 & 0 & 0 & 1 & 0 \\ 38 & 13 & 107 & 45 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In this example, since the eigenvalue $\lambda = 1$ has multiplicity 4 (see Table 3), the code dimension is $k = 4$. The code has minimum distance $d = 5$ and is denoted by $\mathbf{FC}_1^1(8, 4, 5)$.

We remark that several aspects concerning the codes described in this section are currently under investigation. The first one is related to the minimum distance. As the result of some preliminary computer simulations, transform codes with minimum distance $d = n - k + 1$ have been found. Moreover, although standard decoding algorithms may be used for the proposed codes, we believe that transform-based decoding algorithms can be developed; once the codewords are eigensequences of a given FFTT, the syndrome of the received word can be obtained by the computation of that transform, which can be made via a fast algorithm, as it happens with Fourier codes, for which the syndrome

computation is done by an FFT [30]. This would permit the application of fast transforms to the context of error control codes [11].

7. Concluding remarks

In this paper, the eigenstructure of the finite field trigonometric transforms was discussed. The eigenvalues were determined for different types of cosine and sine transform matrices defined over finite fields. New propositions and conjectures were presented and, additionally, systematic procedures for constructing eigenvectors of the referred transform matrices were introduced. Analogies with the real-valued trigonometric transforms eigenstructures were indicated as well as particularities concerning the finite field scenario.

Two potential applications for the developed theory were presented. With respect to sequence separation, its effective application to multiuser communication requires a detailed analysis of factors such as the presence of noise in a channel and the non-simultaneous transmission of information coming from different users. However, even though the above mentioned aspects are not the focus of this paper, we believe that the ideas discussed in Section 6.1 represent the essential basis for further investigations about those communication schemes.

Regarding the proposed transform codes, this work contributes with another link between error control coding and signal processing. In order to clarify such a relationship, the parameters of linear block codes constructed from different types of transform matrices have been investigated. Particularly, we are interested in characterizing the family of codes obtained from the FFTT matrices. Another topic to be investigated is the construction of finite field transforms from well known linear codes, such as Hamming and Golay codes for instance, i.e., the development of the reverse procedure to the one proposed in this paper.

Acknowledgement

The authors would like to acknowledge the insightful comments and suggestions from Prof. H.M. de Oliveira.

References

[1] J.M. Pollard, The fast Fourier transform in a finite field, Math. Comp. 114 (1971) 82–100.
[2] T. Toivonen, J. Heikkilä, Video filtering with Fermat number theoretic transforms using residue number system, IEEE Trans. Circuits Systems Video Tech. 16 (2006) 92–101.
[3] R.M. Campello de Souza, H.M. de Oliveira, A. Kauffman, A.J.A. Paschoal, Trigonometry in finite fields and a new Hartley transform, in: Proceedings of the IEEE International Symposium Information Theory, 1998, pp. 293.
[4] F. Fekri, S.W. McLaughlin, R.M. Mersereau, R.W. Schafer, Block error correcting codes using finite-field wavelet transforms, IEEE Trans. Signal Process. 54 (2006) 991–1004.
[5] K.S. Chan, F. Fekri, A block cipher cryptosystem using wavelet transforms over finite fields, IEEE Trans. Signal Process. 52 (2004) 2975–2991.
[6] J.B. Lima, R.M. Campello de Souza, New trigonometric transforms over prime finite fields for image filtering, in: Proceedings of the International Telecommunications Symposium, Fortaleza, Brazil, 2006, pp. 23–28.
[7] R.E. Blahut, Fast Algorithms for Digital Signal Processing, Addison-Wesley Reading, 1985.
[8] J.B. Lima, R.M. Campello de Souza, D. Panario, Blind sequence separation based on the eigenstructure of finite field transforms, in: Proceedings of the Brazilian Telecommunications Symposium, Rio de Janeiro, Brazil, 2008
[9] R. Bracewell, The Fourier Transform and its Applications, third ed., McGraw-Hill, New York, 1999.
[10] N.S. Rubanov, E.I. Bovbel, P.D. Kukharchik, V.J. Bodrov, The modified number theoretic transform over the direct sum of finite fields to compute the linear convolution, IEEE Trans. Signal Process. 48 (1998) 813–817.
[11] R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, 1983.
[12] S.A. Martucci, Symmetric convolution and the discrete sine and cosine transforms, IEEE Trans. Signal Process. 42 (1994) 1038–1051.
[13] M.M. Campello de Souza, H.M. de Oliveira, R.M. Campello de Souza, M.M. Vasconcelos, The discrete cosine transform over prime finite fields, in: J.N. de Souza, P. Dini, P. Lorenz (Eds.), International Conference on Telecommunications, Lecture Notes in Computer Science (LNCS), vol. 3124, Springer, Berlin, 2004, pp. 482–487.
[14] R.M. Guralnik, M. Lorenz, Orders of finite groups of matrices, in: Groups, Rings and Algebras: Proceedings of a Conference in Honor of Donald S. Passman, Contemporary Mathematics, vol. 420, 2006, pp. 141–162.
[15] D.T. Birtwistle, The eigenstructure of the number theoretic transforms, Signal Process. 4 (1982) 287–294.

[16] J.H. McClellan, T.W. Parks, Eigenvalue and eigenvector decomposition of the discrete Fourier transform, IEEE Trans. Audio Electroacoust. AU-20 (1972) 66–74.
[17] S.-C. Pei, M.H. Yeh, The discrete fractional cosine and sine transforms, IEEE Trans. Signal Process. 49 (2001) 1198–1207.
[18] C.-C. Tseng, Eigenvalues and eigenvectors of generalized DFT, generalized DHT and DST-IV matrices, IEEE Trans. Signal Process. 50 (2002) 866–877.
[19] R.M. Campello de Souza, H.M. de Oliveira, Eigensequences for multiuser communication over the real adder channel, in: Proceedings of the International Telecommunications Symposium, Fortaleza, Brazil, 2006, pp. 989–994.
[20] G. Cariolaro, T. Erseghe, P. Kraniauskas, The fractional discrete cosine transform, IEEE Trans. Signal Process. 50 (2002) 902–911.
[21] J. Konvalina, V. Matache, Palindrome-polynomials with roots on the unit circle, Math. Rep. Acad. Sci. Roy. Soc. Can. 26 (2004) 39–44.
[22] J. von zur Gathen, D. Panario, Factoring polynomials over finite fields: a survey, J. Symbolic Comput. 31 (2001) 3–17.
[23] G.Z. Karabulut, D. Panario, A. Yongaçoglu, Integer to integer Karhunen Loève transform over finite fields, in: Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Montreal, Canada, 2004, pp. 213–216.
[24] V. Ipatov, Spread Spectrum and CDMA Principles and Applications, Wiley, 2005.
[25] H. Schulze, C. Lnders, Theory and Applications of OFDM and CDMA, Wiley, 2005.
[26] B. Nazer, M. Gastpar, Computation over multiple-access channels, IEEE Trans. Inform. Theory 53 (2007) 3498–3516.
[27] S.C. Chan, K.L. Ho, Direct method for computing sinusoidal transforms, IEEE Proc. 137 (1990) 433–442.
[28] J.G. Proakis, Digital Communications, fourth ed., McGraw Hill, 2000.
[29] H.M. de Oliveira, R.M. Campello de Souza, Orthogonal multilevel spreading sequence design, in: P.G. Farnell, M. Darnell, B. Honary (Eds.), Coding, Communications and Broadcasting, Research Studies Press, John Wiley, Hertfordshire, 2000, pp. 291–303.
[30] R.M. Campello de Souza, E.S.V. Freire, H.M. de Oliveira, Fourier codes, in: Proceedings of the 10th International Symposium on Communication Theory and Applications, Ambleside, UK, 2009, pp. 370–375.
[31] S. Lin, D.J. Costello Jr., Error Control Coding, Pearson Prentice-Hall, 2004.